Shibboleth®

Web Single Sign-On and Federating Software

Shibboleth ® software provides Single Sign-On convenience for your users on campus or across the web. The approach to policy-driven authentication and authorization enables you to maintain control over your institution's data and the user's privacy. And your service providers retain control over who accesses their resources and don't have to worry about maintaining up-to-date account information for your user community.

What's the Shibboleth Advantage?

Single Sign-On for Campus and External Services

More and more, universities, companies and government agencies offer services and collaborate online. The user typically accesses both online resources inside and outside their organization to do their work. For example, students log into a learning management system and link to a campus project wiki space and a licensed homework site hosted by a third-party service provider.

In the past, each of these services required its own ID and password and, for the user, that meant adding another set of credentials to that collection of sticky notes. For the institution, closing the security holes and just keeping up with the access changes for the services on and off campus was quite a challenge.

Shibboleth was developed specifically to address these challenges. An individual uses his or her campus userid and password to access resources offered by the institution and provider organizations. And campus IT shops can use their authentication technology of choice — Shibboleth sits on top and provides the web single sign-on functionality.

Build and Manage Locally, Access Globally

But it's not just about single sign-on. Because Shibboleth leverages the local identity and access management system, the net effect is that the individual's relationships with the institution determine the person's access rights to services, hosted both on and off campus. If you build your identity and access management system for campus applications, chances are you can use it for federated third-party ones too.

Protect Your Data and Users' Privacy

With Shibboleth, the campus manages authentication of their users, but the service provider decides whether the individual can access the resource. The campus sends just the minimal data that the provider needs for authorization
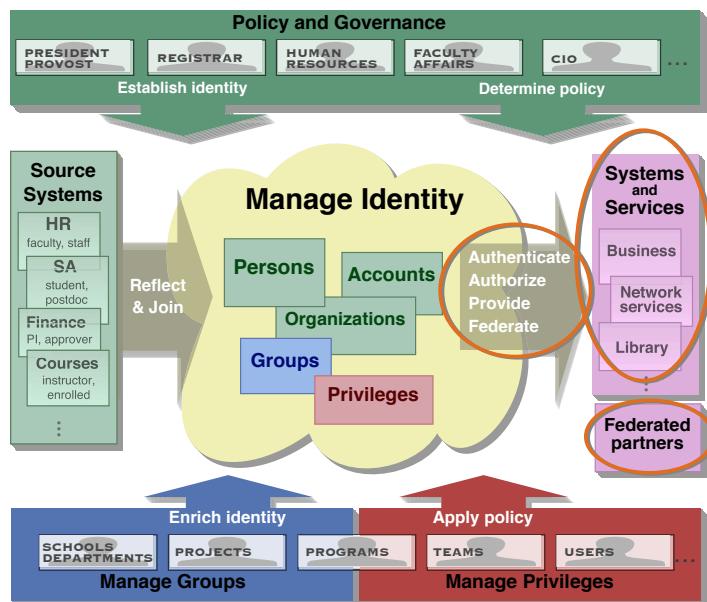
and nothing more. For example, if the name of a student isn't the main criterion for access, but current enrollment in a particular Biology course is, then that is what is sent. And all this is done at the time the user accesses the resource, so the data is delivered just-in-time and governed by policy, according to your institution's approach to privacy.

Partner with your Service Providers

From a service provider's point of view, Shibboleth can substantially reduce the risk and time involved in offering services. In the past, IT departments sent large files of identity data to a service provider to create and update separate accounts. Now, using Shibboleth, the provider receives the information- each time the user accesses the resource—they don't need to maintain campus identity data that goes out of date. And the provider still has control over access to its protected services without the concerns of potential spills of your campus data or miss-configured IP-based access methods.

Join the Federation

While Shibboleth supports setting up agreements, policies, practices, and technology interactions with each separate partner or collaborator, the staff burden decreases and the return on investment increases if you leverage the same set-up again and again with each new partner. A federation provides a standard approach to policies, practices, and technologies that all members, institutions and service providers alike, adopt. Once this "infrastructure" is established, members of the federation can set up new relationships with each other quickly and easily.

Which federation(s) you join should be determined by your business needs and collaborating partners. For example, you might have a federation associated with your state higher-education system for sharing services or contracted resources. You might also have service providers that are members of the InCommon Federation (www.incommonfederation.org) that serves the US Higher Education community and its partners. Think of a federation as a trust infrastructure for collaboration.

From the Government and Here to Help

The Federal Government established the U.S. Federal E-Authentication Federation that comprises many of the government agencies with which campus constituencies work. For instance, faculty often interact with granting agencies, both during the proposal solicitation and grant management stages, and students access loan-related services at the Department of Education. The InCommon and E-authentication Federations are working to develop a framework for inter-federated operation and provide the policy and technical base to allow members to use their campus-issued credentials to access government web-based services.

Plays Well with Others

In a federated world, where commercial sites and U.S. government agencies might be using different federating software—but need to work together—interoperability is extremely important. Shibboleth offers multi-protocol sup-

port that ensures that it will interoperate with other commercial implementations. These protocols include OASIS SAML (versions 1.0, 1.1, and 2.0), protocols and extensions for Microsoft's Active Directory Federation Services and, in the future, CardSpace.™

How Do I Get Started?

To learn more about the Shibboleth authentication and federating software, visit the Shibboleth website (.shibboleth.internet2.edu). You can become active in the community by joining email lists and attending the workshops and presentations offered around the country. To get started with identity management infrastructures, refer to our NSF-funded project NMI-EDIT at www.nmi-edit.org, which offers roadmaps, practice papers, articles and other tools to get you going.

About the Internet2 Middleware Initiative

Led by the Middleware Architecture Committee for Education (MACE), the Internet2 Middleware Initiative comprises a number of projects that address challenges in the middleware space, such as identity and access management. For more information, visit middleware.internet2.edu.

> *At Ohio State, we believe that the ability to provide trusted authentication across different organizations is an essential requirement for today's course management systems. We're working with other universities, as well as our library, to offer single sign-on capabilities to diverse and distributed student populations with the course management system as the front door to these integrated services.*
>
> *Steve Acker*
> *Director of Learning Technologies*
> *Research and Innovation*
> *The Ohio State University*

shibboleth.internet2.edu

200706-IS-Shib